UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/659,834	09/10/2003	Tamio Saito	7167-102.US/10311148	5947

167 7590 11/16/2004

FULBRIGHT AND JAWORSKI L L P
PATENT DOCKETING 29TH FLOOR
865 SOUTH FIGUEROA STREET
LOS ANGELES, CA 900172576

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 11/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/659,834	SAITO ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☒ Claim(s) *11,15,16 and 24* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 11, 15, 16, and 24 are objected to because of the following informalities:

- Regarding claims 11 and 16, these claims are the same and depend from the same claim. Please remove one of these claims and correct the numbering of the remaining claims. Remember the numbering has to be successive numbering with no missing numbers.
- Regarding claim 15, the claim is missing the dependent claim number that it depends from. Examiner treats claim 15 as being dependent upon claim 14.
- Regarding claim 24, the claim misplaced "at least some of the captured" at the end of the claim. It should be "...means for restricting at least some of the captured use of the card...".

Appropriate correction is required.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-8, 18-20, 24, 25, 27, and 28 are rejected under 35 U.S.C. 102(b) as being anticipated by Shen (E.P. No. 1,074,949).

Regarding claim 1, Shen teaches an intelligent identification card comprising:

- An on-board memory for storing reference data (fig. 1, ref. num 11),
- An on-board sensor for capturing live biometric data (fig. 1, ref. num 12),
- An on-board microprocessor for comparing the captured biometric data with corresponding stored reference data within a predetermined threshold and for generating a verification message only if there is a match within a predetermined threshold (fig. 1, ref. num 14), and
- Means for communicating the verification message to an external network (fig. 1, ref. num 13).

Regarding claim 2, Shen teaches wherein the verification message includes at least excerpts from the stored reference data (col. 3, lines 31-36).

Regarding claim 3, Shen teaches wherein the verification message includes at least excerpts from the captured biometric data (col. 3, lines 31-36).

Regarding claim 4, Shen teaches wherein the verification message is transmitted to a remote authentication system for additional verification (col. 3, lines 31-36).

Regarding claim 5, Shen teaches wherein the remote authentication system includes remotely stored reference data that is different from the locally stored reference data (col. 3, lines 28-31).

Regarding claim 6, Shen teaches wherein the on-board microprocessor uses a different matching algorithm than that used at the remote authentication system (col. 4, lines 3-8).

Regarding claim 7, Shen teaches wherein the entire matching process is performed by the on-board processor and none of the captured biometric data is transmitted to the network (col. 3, lines 31-36).

Regarding claim 8, Shen teaches wherein both the originally captured biometric data and any other "private" information stored in the on-board memory are not made available to any external processes (col. 3, lines 25-31).

Regarding claim 18, Shen teaches wherein the biometric data includes fingerprint data and the sensor is a fingerprint sensor which captures data from a user's finger placed on the sensor (col. 3, lines 9-11).

Regarding claim 19, Shen teaches wherein real-time feedback is provided while the user is manipulating his finger over the fingerprint sensor, thereby facilitating an optimal placement of the finger over the sensor (col. 4, lines 18-23).

Regarding claim 20, Shen teaches wherein the matching process utilizes a hybrid matching algorithm that takes into account both minutiae and overall spatial relationships in the captured biometric data (col. 3, lines 42-57).

Regarding claim 24, Shen teaches wherein the card further comprises means for restricting at least some of the captured use of the card to a predetermined location (col. 1, lines 6-14).

Regarding claim 25, Shen teaches wherein at least some of the captured biometric data and the reference data are transmitted to a separate authentication server for secure verification of a user's identity priori to any grant of on-line access to an application server for processing of secure financial transactions involving that user (col. 3, lines 28-36).

Regarding claim 27, Shen teaches wherein the output from the card is used to obtain physical access into a secure area (col. 1, lines 9-12).

Regarding claim 28, Shen teaches wherein a record of successful and unsuccessful access attempts is maintained on the card (col. 4, lines 8-17).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 9, 10, 14, 15, 17, 21-23, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shen (E.P. No. 1,074,949) in view of DiGiorgio et al. (U.S. Patent No. 6,385,729).

Regarding claim 9, Shen teaches all the limitations of claims 1 and 2, above. However, Shen does not teach wherein the card is ISO Smartcard compatible.

DiGiorgio et al. teaches wherein the card is ISO Smartcard compatible (col. 4, line 53 through col. 5, line 12).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine the card is ISO compatible, as taught by DiGiorgio et al., with the card of Shen. It would have been obvious for such modifications because

ISO compatible cards are already defined by a standard; acceptance of the card would be come easier than trying to define a new card standard.

Regarding claim 10, the combination of Shen in view of DiGiorgio et al. teaches further comprising an ISO Smartcard processor (see col. 4, line 53 through col. 5, line 12 of DiGiorgio et al.).

Regarding claim 17, the combination of Shen in view of DiGiorgio et al. teaches wherein:

- The card comprises an upper magnetic stripe region and a lower embossed region (see fig. 2B, ref. num 22 of DiGiorgio et al.);
- The biometric sensor is a fingerprint sensor (see col. 3, lines 9-12 of Shen); and
- The security processor, the ISO Smartcard processor and the fingerprint sensor are all located in a middle region between the upper region and the lower region (see fig. 1 of Shen).

Regarding claims 14 and 15, the Examiner takes official notice that the security processor has a first connection used for loading data during a loading process and a second connection connected to an external network and the first connection is permanently disabled after the loading process has been completed.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine two connections on the card, one that is disabled after the initial loading is completed. It would have been obvious for such modifications because the second connection provides I/O to the network exclusively, while the first connection can be used specifically for one purpose, then disabled to not allow any other data to be placed on the card; such data may overwrite the stored data, thereby defeating the security of the card.

Regarding claims 21-23, Shen teaches all the limitations of claims 1, 2, and 18, above. However, Shen does not teach wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate, the backing plate comprises a glass epoxy layer sandwiched between two metal layers, and the backing plate is reinforced by a carrier frame surrounding the sheet of silicon.

DiGiorgio et al. teaches wherein the fingerprint sensor comprises a sheet of crystalline silicon supported by a backing plate, the backing plate comprises a glass epoxy layer sandwiched between two metal layers, and the backing plate is reinforced by a carrier frame surrounding the sheet of silicon (col. 5, lines 58-63).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine a silicon fingerprint sensor, epoxy backing, and reinforcing the backing by a carrier frame, as taught by DiGiorgio et al., with the card of

Shen. It would have been obvious for such modifications because the materials used provide tamper resistance, which prevents the data inside –mainly the stored biometrics and credit card information– from being compromised should the smart card be disassembled.

Regarding claim 26, Shen teaches all the limitations of claims 1 and 25, above. However, Shen does not teach wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid.

DiGiorgio et al. teaches wherein in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed in which a challenge character sequence is sent from the authentication sever to the identification card as, the identification card then uses the challenge character sequence and the match request to generate a challenge response which it then

forwards to the application server, the application server then forwards the challenge response to the authentication server, which then verifies whether the challenge response is valid (col. 10, lines 24-53).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine in response to a match request relating to a particular logon attempt at a particular application server which produces a positive match at the authentication server, a secure three-way authentication protocol is executed which verifies whether the challenge response is valid, as taught by DiGiorgio et al., with the card of Shen. It would have been obvious for such modifications because challenge/response systems allow devices to verify a secret without having to exchange the secret in the clear. It would be useful to do this because the devices can ensure security without having to establish a common secret beforehand.

Claims 11-13 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shen (E.P. No. 1,074,949) in view of DiGiorgio et al. (U.S. Patent No. 6,385,729), and further in view of Goldwasser et al. (U.S. Patent No. 4,926,479).

Regarding claims 11-13 and 16, the combination of Shen in view of DiGiorgio et al. teaches all the limitations of claims 1, 2, 9, and 10, above. However, the combination of Shen in view of DiGiorgio et al. does not teach wherein the security processor used for storing and processing the protected biometric data is functionally

separated from the ISO Smartcard processor by a firewall, all external data to and from the security processor passes through the ISO Smartcard processor, all external data to and from the ISO Smartcard processor passes through the security processor, and the security processor used for storing and processing the protected biometric data is functionally separated from the ISO Smartcard processor by a firewall.

Goldwasser et al. teaches wherein the security processor used for storing and processing the protected biometric data is functionally separated from the ISO Smartcard processor by a firewall (col. 10, lines 45-56), all external data to and from the security processor passes through the ISO Smartcard processor (col. 10, lines 57-60), and all external data to and from the ISO Smartcard processor passes through the security processor (col. 10, lines 57-60).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine separating the two processors by a firewall and causing all communications in and out of one processor to go through the other processor, as taught by Goldwasser et al., with the card of Shen/DiGiorgio et al. It would have been obvious for such modifications because two processors can solve different tasks. This allows application specific tasks to be performed by the better processor.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoffman

BH

AYAZ SHEIKH
VISORY PATENT EXAMINER
NOLOGY CENTER 2100